PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-331750

(43)Date of publication of application : 30.11.2001

(51)Int.Cl. G06F 17/60
A63F 7/02
G06K 17/00
G07F 7/12

(21)Application number : 2000-151223

(22)Date of filing : 23.05.2000

(71)Applicant : SAWATAKE KAZUO
WATABE TERUO

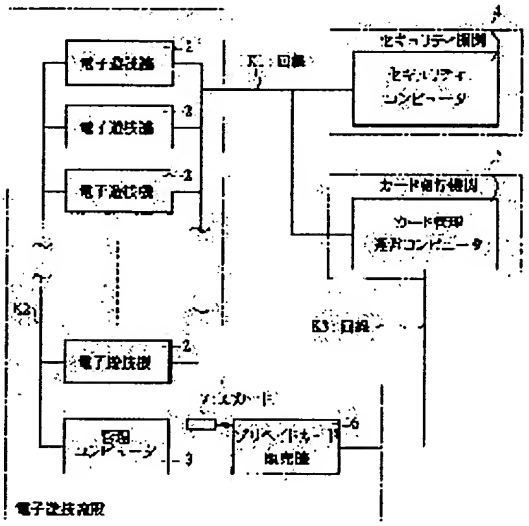
(72)Inventor : SAWATAKE KAZUO

(54) PREPAID CARD COLLATION SYSTEM AND ELECTRONIC GAME MANAGEMENT SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To surely prevent others from wrongfully using a prepaid card and to effectively suppress wrongs to an electronic game machine.

SOLUTION: When purchasing the prepaid card, a user inputs his or her fingerprint information and a password from a prepaid card vending machine 6. This information is stored in a card management operation computer 5 and an IC card 7 as security data together with an authentication number of the IC card 7. When playing an electronic game machine 2, the user inserts the IC card 7 to the electronic game machine 2 and inputs fingerprint information and the password from the electronic game machine 2. A security communication control part of the electronic game machine 2 takes in security data registered in the computer 5 and collates this security data, security data inputted from the electronic game machine 2, and security data of the IC card 7 with one another, and use of the IC card 7 is permitted if they coincide with one another.



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]Especially this invention is applied to user collation of the IC card used for electronic recreation facilities etc. about the unauthorized use prevention art of a prepaid card, and relates to effective art.
[0002]
[Description of the Prior Art]For example, in recreation facilities, such as pachinko, using the prepaid card purchased beforehand as a case where a user receives the loan of a game ball is known widely.
[0003]According to the place which this invention person examined, the prepaid card is put on the market with the ticket machine in recreation facilities, etc., for example. A game ball is automatically lent out by inserting this prepaid card in the card unit provided in the game machine after the user purchased the prepaid card of the expectation from the ticket machine, and a game machine's carrying out ball lending and pushing a button.
[0004]A game advances according to the game program memorized by ROM (Read Only Memory) etc. by which the game machine was generally formed in the inside according to a user's operation.
[0005]
[Problem(s) to be Solved by the Invention]However, it was found out by this invention person in the loan art of the game ball by the above prepaid cards that there are the following problems.
[0006]That is, in a prepaid card, since a user cannot check whether you are the person himself/herself who purchased this prepaid card, when a prepaid card is lost, there is a possibility that it may be used for others, for example.
[0007]A prepaid card is generally a magnetic card and various data of the balance etc. is memorized as magnetic data. This sake. There is also a possibility that the prepaid card in

which magnetic data was altered may be used improperly.

[0008]A game machine is difficult to recognize that the malfeasance is performed, when a certain specific operation is performed and unjust program correction, such as considering it as a big hit situation, is carried out, for example, since a game advances according to a game program as mentioned above.

[0009]The purpose of this invention is to provide the prepaid card collation system and electronic game control system which can prevent the unauthorized use of the prepaid card by others certainly, and can control the malfeasance of an electronic game machine effectively.

[0010]

[Means for Solving the Problem]A prepaid card collation system of this invention is connected to a network, A prepaid card issuing means which writes security data inputted by user in this prepaid card, and publishes it when purchasing a prepaid card, A data storing means which stores security data which was connected to a network and inputted from a prepaid card issuing means via the network, It is connected to a network, Security data inputted when a user uses a prepaid card, security data incorporated from a prepaid card issuing means via a network, and security data incorporated from said data storing means via a network are compared, Only when these three security data agreed, it had a card use means to permit use of a prepaid card.

[0011]A prepaid card collation system of this invention, The 1st security data input part into which a user's security data is inputted for said prepaid card issuing means, A data read part which reads a service number beforehand stored in a prepaid card, It has a data writing part which writes security data inputted from the 1st security data input part in said prepaid card, A security data read part from which said card use means reads security data of a prepaid card, The 2nd security data input part into which a user's security data is inputted, Security data incorporated from a data storing means, and security data read from a prepaid card, Only when security data inputted from the 2nd security data input part was compared and these three security data agreed, it had a comparison control section which permits use of a prepaid card.

[0012]A prepaid card collation system of this invention, Security data inputted from said 1st and 2nd security data input part, Security data which is a user's fingerprint information and a password and is stored in said data storing means, It is characterized by being a service number of a prepaid card read to fingerprint information, a password, and a data read part of a user inputted from the 1st security data input part.

[0013]An electronic game control system of this invention is connected to a network, A prepaid card issuing means which writes security data inputted by user in a prepaid card, and publishes it when purchasing a prepaid card used with electronic recreation facilities, A data storing means which stores security data which was connected to a network and inputted from

a prepaid card issuing means via the network, It is connected to a network, Via security data and a network which are inputted when a user uses a prepaid card in electronic recreation facilities. Security data incorporated from a prepaid card issuing means and security data incorporated from a data storing means via a network are compared, Only when these three security data agreed, it had with an electronic game machine which formed a card use means to permit use of a prepaid card.

[0014]The 1st security data input part to which a user's security data is inputted into an electronic game control system of this invention for said prepaid card issuing means, A data read part which reads a service number beforehand stored in a prepaid card, It has a data writing part which writes security data inputted from the 1st security data input part in a prepaid card, A security data read part from which said card use means reads security data of a prepaid card, The 2nd security data input part into which a user's security data is inputted, Security data inputted from security data incorporated from a data storing means, security data read from a prepaid card, and the 2nd security data input part is compared, Only when these three security data agreed, it had a comparison control section which permits use of a prepaid card.

[0015]Security data into which an electronic game control system of this invention is inputted from said 1st and 2nd security data input part, Security data which is a user's fingerprint information and a password and is stored in said data storing means, It is characterized by being a service number of a prepaid card read by fingerprint information, a password, and a data read part of a user inputted from the 1st security data input part.

[0016]An electronic game control system of this invention to said electronic game control system. When it is connected to a network and a detection signal is inputted via a network, Have a security control means to reply a diagnostic program which diagnoses a game program stored in an electronic game machine, and to said electronic game machine. Detect that a power supply was supplied to an electronic game machine, and a detection signal is outputted to security via a network, When a game program was diagnosed with a diagnostic program returned from a security control means and a diagnostic result had fault, a detection control section which outputs an abnormal signal to a security control means was provided.

[0017]An electronic game control system of this invention eliminates a diagnostic program with which said detection control section is replied from a security control means for every end of diagnostic.

[0018]An electronic game control system of this invention is connected to a network, A security control means to reply a diagnostic program which diagnoses a game program stored in an electronic game machine when a detection signal is inputted via the network, Detect that a power supply was supplied to an electronic game machine, and a detection signal is outputted to security via a network, When a game program was diagnosed with a diagnostic program

returned from a security control means and a diagnostic result had fault, it had an electronic game machine which provided a detection control section which outputs an abnormal signal to this security control means.

[0019]An electronic game control system of this invention eliminates a diagnostic program with which said detection control section is replied from a security control means for every end of diagnostic, and a security control means is changed whenever it replies the contents of the diagnostic program.

[0020]the time of using a prepaid card by the above thing -- three security data -- since it compares, an unauthorized use of this prepaid card can be prevented certainly in a short time.

[0021]If a power supply is supplied to an electronic game machine, an unauthorized use of a game program, etc. can be discovered and prevented with a diagnostic program, without applying a working man hour etc., since the automated diagnosis of the game program is carried out.

[0022]

[Embodiment of the Invention]Hereafter, an embodiment of the invention is described in detail based on a drawing.

[0023]The explanatory view of the composition in the electronic game system by the 1 embodiment of this invention and drawing 2 drawing 1, The explanatory view of the electronic game machine in the electronic game system by the 1 embodiment of this invention and drawing 3, The flow chart in the electronic game system at the time of purchasing an IC card from the prepaid card vending machine by the 1 embodiment of this invention and drawing 4, The flow chart in the electronic game system at the time of the user by the 1 embodiment of this invention playing with an electronic game machine and drawing 5 are the flow charts in the electronic game system at the time of performing the security check of the electronic game machine by the 1 embodiment of this invention.

[0024]In this embodiment, the electronic game system (electronic game control system) 1, it is shown in drawing 1 -- as -- two or more electronic game machines (a prepaid card collation system.) the card use means 2, the management computer 3, the security computer (security control means) 4, and a card management management computer (a prepaid card collation system.) It comprises the data storing means 5 and the prepaid card vending machine (a prepaid card collation system, a prepaid card issuing means) 6.

[0025]Two or more electronic game machines 2, the management computer 3, and the prepaid card vending machine 6 are formed in electronic recreation facilities among the electronic game systems 1. The organization which performs security managements, such as a program of the electronic game machine 2, has the security computer 4, and card issuing machine Seki etc. which publish IC card (prepaid card) 7 have the card management management computer 5. It is connected also with the electronic game machine with which the security computer 4

and the card management management computer 5 are formed out of electronic recreation facilities, and these are provided in other electronic recreation facilities.

[0026]A game advances based on the stored game program, the game of the electronic game machine 2 is played using IC card 7 which a user mentions later, and the value according to a game result is given.

[0027]IC card 7 consists of composition that, for example, the semiconductor chip and the antenna linked to it were incorporated into the card, catches the electric wave which this antenna discharges from a unit and the semiconductor chip in a card, and exchanges the information in a card.

[0028]The security data which a user inputs at the time of purchase, management data, etc. are stored in IC card 7. Security data is a password which a user enters, the identification numbers (or the serial number of IC card 7, a specific number, etc.) beforehand stored in the IC card, fingerprint information, etc., and management data is a card point etc.

[0029]The security computer 4 is connected to the electronic game machine 2 via the circuits (network) K1, such as a dedicated line and a telephone line, at on-line, and an exchange of the data of the diagnostic program etc. which diagnose the program injustice of the electronic game machine 2, etc. is performed.

[0030]The management computer 3 is connected to the electronic game machine 2 via the circuits K2, such as LAN, respectively. The management total of the operating ratio of the electronic game machine 2, sales, etc. is managed, the security computer 4 supervises the operating condition of the electronic game machine 2, and the management computer 3 prevents an unauthorized use.

[0031]The circuit K1 is connected also to the card management management computer 5, and this card management management computer 5 stores the security data inputted, management data, etc., when a user purchases IC card 7.

[0032]The card management management computer 5 is connected to the prepaid card vending machine 6 via the circuits (network) K3, such as a dedicated line or a telephone line. In this prepaid card vending machine 6, a fingerprint sensor (the 1st security data input part), An input part (the 1st security data input part), data read / write-in function (a data read part, a data writing part) is provided also with the function which outputs the security data had and inputted and management data to the card management management computer 5.

[0033]A fingerprint sensor incorporates a user's own fingerprint as fingerprint information, when a user purchases IC card 7. An input part consists of a display, a keyboard, or a touch input panel with which they were united, and when a user similarly purchases IC card 7, it inputs the information on a password etc. Data read / write-in function is functions which write security data etc. in IC card 7, or read management data.

[0034]The circuitry of the electronic game machine 2 is explained.

[0035]the electronic game machine 2 is shown in drawing 2 -- as -- the fingerprint sensor (the 2nd security data input part) 8, the card read/write part (security data read part) 9, the password input part (the 2nd security data input part) 10, and a security communication control section (a comparison control section.) It comprises the detection control section 11, the game main control section 12, the game program storing media drive 13, the I/O part 14, the power supply unit 15, the indicator 16, and the switch panel part 17.
[0036]The security communication control section 11 is connected to the fingerprint sensor 8 and the card read/write part 9. The fingerprint sensor 8 is incorporated as fingerprint information, such as a user's fingerprint. The card read/write part 9 reads or writes in the data memorized by IC card 7.
[0037]The security communication control section 11 is connected to the security computer 4 and the card management management computer 5 via the circuit K1. The security communication control section 11 performs motion control of the game main control section 11 based on the collated result of IC card 7, the fingerprint sensor 8, and security data, or the diagnostic result of the diagnostic program outputted from the security computer 4.
[0038]The security communication control section 11, the game program storing media drive 13, the I/O part 14, etc. are connected to the game main control section 12.
[0039]The game main control section 12 manages control of the game progress of the electronic game machine 2, etc. based on a game program. The game program storing media drive 13, For example, it is a CD-ROM (Compact Disc Read Only Memory) drive, a DVD (Digital Video Disc)-ROM drive, etc., and the game program recorded on CD-ROM, DVD-ROM, etc. is read. The management computer 3 is connected to the I/O part 14, and data is outputted and inputted via this I/O part 14.
[0040]While the power supply unit 15 supplies the optimal power supply for the fingerprint sensor 8, the card read/write part 9, the security communication control section 11, the game main control section 12, the game program storing media drive 13, the I/O part 14, the indicator 16, and the switch panel part 17, When a power supply is supplied to the electronic game machine 2, a seizing signal is outputted to the security communication control section 11.
[0041]The game main control section 12 is connected to the indicator 16 and the switch panel part 17, respectively. The indicator 16 consists of a liquid crystal display, a cathode-ray tube, etc., for example, and the picture for game plays is displayed. The switch panel part 18 has final controlling elements, such as a switch for game plays, and a keyboard for data input.
[0042]Next, operation of the electronic game system in this embodiment is explained using the flow chart of drawing 1, drawing 2 and drawing 3 - drawing 5.
[0043]First, when a user purchases an IC card. As shown in drawing 3, a price is injected into the prepaid card vending machine 6, a user's own finger is forced on the fingerprint sensor

with which the prepaid card vending machine 6 was equipped, fingerprint information is inputted, and a password is entered from the input part of the prepaid card vending machine 6 (Step S101).

[0044]A user's inputted fingerprint information and a password are written in IC card 7 by the data read / write-in function of the prepaid card vending machine 6, and are memorized as security data with the service number beforehand given to each IC card 7, respectively (Step S102).

[0045]The arbitrary point data which a user wishes to have with the data read / write-in function of the prepaid card vending machine 6 (purchase) are memorized by IC card 7 (Step S102).

[0046]Simultaneously, the prepaid card vending machine 6 reads the service number of IC card 7 with data read / write-in function, and outputs the security data which consists of this service number, a user's fingerprint information, and a password to the card management management computer 5.

[0047]The card management management computer 5 stores the transmitted security data in a database etc. (Step S103). An end of these operations will publish IC card 7 from the prepaid card vending machine 6 (Step S104).

[0048]While inserting purchased IC card 7 in the card read/write part 9 of the electronic game machine 2 as shown in drawing 4 when a user plays with the electronic game machine 2, the same finger as the fingerprint registered at the time of the purchase of IC card 7 is forced on the fingerprint sensor 8 of the game machine 2 (Step S201).

[0049]The card read/write part 9 reads security data and management data from inserted IC card 7, and outputs them to the security communication control section 10 (Step S202).

[0050]The fingerprint sensor 8 incorporates a user's fingerprint information, and outputs it to the security communication control section 10 (Step S203). A user enters the password entered when IC card 7 was purchased from the password input part 10 of the electronic game machine 2 (Step S204).

[0051]At this time, the security communication control section 10 incorporates the security data inputted from the prepaid card vending machine 6 from the database of the card management management computer 5 (Step S205). The turn of processing may interchange or it may be made for processing of Steps S202-S205 to process all simultaneously here.

[0052]and the security data (the fingerprint information which the fingerprint sensor 8 incorporated.) into which the security communication control section 10 was inputted from the electronic game machine 2 The password entered from the password input part 10, the security data of IC card 7 which the card read/write part 9 read, and the security data incorporated from the database of the card management management computer 5 are compared (Step S206).

[0053]When these security [all] data has agreed, it attests that a user is the person

himself/herself, the security communication control section 10 permits use of IC card 7, and the control signal which starts a game to the game main control section 12 is outputted (Step S207).

[0054]In response to this signal, the game main control section 12 requires the point for games. In processing of Step S207, when security data is not in agreement, the security communication control section 10 controls to discharge the IC card 7 compulsorily from the card read/write part 9 (Step S208).

[0055]If the point for games is required, a user will do the injection directions of the arbitrary points from the switch panel part 19 etc. (Step S209), and a game will be started.

[0056]The point in which injection directions were done by the user is transmitted to the card management management computer 5 via the security communication control section 11, and the point by which injection directions were carried out is subtracted from the management data stored in the database of the card management management computer 5, and the management data of IC card 7. When the point for games is lost during a play, a user does the injection directions of the arbitrary points from the switch panel part 19 etc. again.

[0057]When ending a game, by pushing the adjustment button provided in the switch panel part 17 etc., adjustment processing of a final point is performed and the point after adjustment processing is newly rewritten by the database of IC card 7 and the card management management computer 5.

[0058]Next, the security check of the electronic game machine 2 at the time of opening of electronic recreation facilities is explained using drawing 5.

[0059]If a power supply is supplied to the electronic game machine 2 (Step S301), a seizing signal will be outputted to the security communication control section 11 from the power supply unit 15. The detection signal which tells the security computer 4 about powering on of the security communication control section 11 having been carried out to the electronic game machine 2 based on the seizing signal is outputted (Step S302).

[0060]The security computer 4 which received the detection signal transmits a diagnostic program to the security communication control section 11 (Step S303), and with the diagnostic program, injustice is given to a game program and it diagnoses whether it is no (Step S304).

[0061]The contents of a program are rewritten every day, it is transmitted, and this diagnostic program can make it impossible as a matter of fact to develop this diagnostic program compatible unjust program.

[0062]In diagnosis of the game program by a diagnostic program, if it is diagnosed that there is no injustice, a diagnostic program will be automatically eliminated by the security communication control section 11 (Step S305), and, in the electronic game machine 2, a game start will be possible.

[0063]If it is judged that a game program has injustice, the security communication control

section 11 will control so that the game main control section 12 does not operate, while outputting an unjust detecting signal to the security computer 4 (Step S306). The security computer 4 which received the unjust detecting signal is notified to the organs concerned of an unjust measure, etc. (Step S307).

[0064]Also when CD-ROM etc. by which the security communication control section 11 was stored in the game program storing media drive 13 are taken out unjustly, Based on the detecting signal outputted from the game program storing media drive 13, an unjust detecting signal is outputted to the security computer 4.

[0065]The security data into which the user of IC card 7 was inputted from the electronic game machine 2 by that cause according to this embodiment, Since it compares by three, the security data stored in the card management management computer 5, and the security data stored in IC card 7, IC card 7 can be managed in real time, and an unauthorized use can be prevented efficiently in a short time.

[0066]The unauthorized use of a game program can be prevented without applying a working man hour by diagnosing automatically whether injustice is given every day to the power up of the electronic game machine 2 at the game program with a daily diagnostic program.

[0067]It cannot be overemphasized that it can change variously in the range which this invention is not limited to said embodiment and does not deviate from the gist.

[0068]For example, although the case where what is called a point addition-and-subtraction type with which the value (point) according to a game result is given of electronic game machine was used as a card use means in said embodiment was indicated, It may be made to use a card use means for a system point subtraction type [, such as shopping by the service from which the point is subtracted in proportion to the hour of use seen by the Internet etc. or a point,].

[0069]

[Effect of the Invention](1) According to this invention, since three security data is compared when using a prepaid card, an unauthorized use can be prevented certainly in a short time, managing this prepaid card in real time.

(2) In this invention, the alteration of a game program, an unauthorized use, etc. can be prevented certainly, without applying a working man hour etc., since the automated diagnosis of the game program is carried out with a diagnostic program whenever a power supply is supplied to an electronic game machine.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]A prepaid card collation system comprising:
A prepaid card issuing means which writes security data inputted by user in said prepaid card, and publishes it when it is connected to a network and a prepaid card is purchased.
A data storing means which stores security data which was connected to said network and inputted from said prepaid card issuing means via said network.
Security data inputted when it is connected to said network and a user uses said prepaid card.
Security data incorporated from said prepaid card issuing means via said network, A card use means to permit use of a prepaid card only when security data incorporated from said data storing means via said network is compared and these three security data agrees.

[Claim 2]A prepaid card collation system comprising:
The 1st security data input part into which a user's security data is inputted for said prepaid card issuing means in the prepaid card collation system according to claim 1.
A data read part which reads a service number beforehand stored in a prepaid card.
A security data read part which is provided with a data writing part which writes security data inputted from said 1st security data input part in said prepaid card and from which said card use means reads security data of said prepaid card.
The 2nd security data input part into which a user's security data is inputted, Security data incorporated from said data storing means, and security data read from said prepaid card, A comparison control section which permits use of a prepaid card only when security data inputted from said 2nd security data input part is compared and these three security data agrees.

[Claim 3]In the prepaid card collation system according to claim 1 or 2, security data inputted

from said 1st and 2nd security data input part, Security data which is a user's fingerprint information and a password and is stored in said data storing means, A prepaid card collation system being a service number of said prepaid card read to fingerprint information, a password, and said data read part of a user inputted from said 1st security data input part.
[Claim 4]An electronic game control system having with an electronic game machine characterized by comprising the following.
A prepaid card issuing means which writes security data inputted by user in said prepaid card, and publishes it when purchasing a prepaid card which is connected to a network and used with electronic recreation facilities.
A data storing means which stores security data which was connected to said network and inputted from said prepaid card issuing means via said network.
It is connected to said network, Via security data inputted when a user uses said prepaid card in electronic recreation facilities, and said network. A card use means to permit use of a prepaid card only when security data incorporated from said prepaid card issuing means and security data incorporated from said data storing means via said network are compared and these three security data agrees.

[Claim 5]An electronic game control system comprising:
The 1st security data input part into which a user's security data is inputted for said prepaid card issuing means in the electronic game control system according to claim 4.
A data read part which reads a service number beforehand stored in said prepaid card.
A security data read part which is provided with a data writing part which writes security data inputted from said 1st security data input part in said prepaid card and from which said card use means reads security data of said prepaid card.
The 2nd security data input part into which a user's security data is inputted, Security data incorporated from said data storing means, and security data read from said prepaid card, A comparison control section which permits use of a prepaid card only when security data inputted from said 2nd security data input part is compared and these three security data agrees.

[Claim 6]In the electronic game control system according to claim 4 or 5, security data inputted from said 1st and 2nd security data input part, Security data which is a user's fingerprint information and a password and is stored in said data storing means, An electronic game control system being a service number of said prepaid card read by fingerprint information, a password, and said data read part of a user inputted from said 1st security data input part.
[Claim 7]An electronic game control system comprising:
In an electronic game control system given in any 1 paragraph of claims 4-6, A security control

means to reply a diagnostic program which diagnoses a game program stored in said electronic game machine when it is connected to said network and a detection signal is inputted into said electronic game control system via said network.
In said electronic game machine, it detects that a power supply was supplied to said electronic game machine, A detection control section which outputs a detection signal to said security via said network, and outputs an abnormal signal to said security control means when a game program is diagnosed with a diagnostic program returned from said security control means and a diagnostic result has fault.

[Claim 8]An electronic game control system, wherein said detection control section eliminates a diagnostic program replied from said security control means for every end of diagnostic in the electronic game control system according to claim 7.
[Claim 9]An electronic game control system comprising:
A security control means to reply a diagnostic program which diagnoses a game program stored in an electronic game machine when it is connected to a network and a detection signal is inputted via said network.
Detect that a power supply was supplied to said electronic game machine, and a detection signal is outputted to said security via said network, An electronic game machine which provided a detection control section which outputs an abnormal signal to said security control means when a game program is diagnosed with a diagnostic program returned from said security control means and a diagnostic result has fault.

[Claim 10]An electronic game control system said detection control section's eliminating a diagnostic program replied from said security control means for every end of diagnostic in the electronic game control system according to claim 9, and changing it whenever a security control means replies the contents of the diagnostic program.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－331750
（P2001－331750A）
(43)公開日　平成13年11月30日(2001.11.30)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ　17/60	４０８	Ｃ０６Ｆ　17/60	４０８	２Ｃ０８８
Ａ６３Ｆ　7/02	３２８	Ａ６３Ｆ　7/02	３２８	３Ｅ０４４
	３３４		３３４	５Ｂ０５５
	３５２		３５２Ｆ	５Ｂ０５８
Ｇ０６Ｋ　17/00		Ｃ０６Ｋ　17/00	Ｒ	

審査請求　未請求　請求項の数10　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願2000－151223(P2000－151223)

(22)出願日　平成12年５月23日(2000.5.23)

(71)出願人　595166697
澤武　一夫
東京都葛飾区柴又３丁目４番12号　イマージ401

(71)出願人　500233371
渡部　照雄
千葉県習志野市谷津６－16－17

(72)発明者　澤武　一夫
東京都葛飾区柴又３－４－12

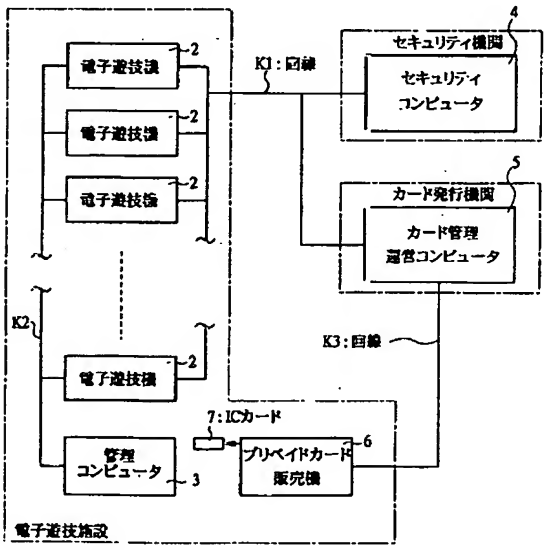
(74)代理人　100080001
弁理士　筒井　大和　（外２名）

最終頁に続く

(54)【発明の名称】　プリペイドカード照合システムおよび電子遊技管理システム

(57)【要約】
【課題】　他人によるプリペイドカードの不正使用を確実に防止し、かつ電子遊技機の不正行為を効果的に抑制する。
【解決手段】　プリペイドカードの購入際に、プリペイドカード販売機６から利用者の指紋情報、パスワードを入力する。その情報はＩＣカード７の認識番号とともにセキュリティデータとしてカード管理運営コンピュータ５、ＩＣカード７に格納される。電子遊技機２をプレイする際には、ＩＣカード７を電子遊技機２に差し込み、かつ電子遊技機２から指紋情報とパスワードとを入力する。電子遊技機２のセキュリティ通信制御部は、カード管理運営コンピュータ５に登録したセキュリティデータを取り込み、このセキュリティデータ、電子遊技機２から入力されたセキュリティデータ、およびＩＣカード７のセキュリティデータを照合し、一致している場合にはＩＣカード７の使用を許可する。

図 1



【特許請求の範囲】

【請求項１】　ネットワークに接続され、プリペイドカードを購入する際に、利用者により入力されたセキュリティデータを前記プリペイドカードに書き込んで発行するプリペイドカード発行手段と、

前記ネットワークに接続され、前記ネットワークを介して前記プリペイドカード発行手段から入力されたセキュリティデータを格納するデータ格納手段と、

前記ネットワークに接続され、利用者が前記プリペイドカードを使用する際に入力されるセキュリティデータと、前記ネットワークを介して前記プリペイドカード発行手段から取り込んだセキュリティデータと、前記ネットワークを介して前記データ格納手段から取り込んだセキュリティデータとを照合し、それら３つのセキュリティデータが合致した場合にだけプリペイドカードの使用を許可するカード使用手段とを備えたことを特徴とするプリペイドカード照合システム。

【請求項２】　請求項１記載のプリペイドカード照合システムにおいて、

前記プリペイドカード発行手段が、

利用者のセキュリティデータが入力される第１セキュリティデータ入力部と、

プリペイドカードに予め格納された認識番号を読み出すデータ読み出し部と、

前記第１セキュリティデータ入力部から入力されたセキュリティデータを前記プリペイドカードに書き込むデータ書き込み部とを備え、

前記カード使用手段が、

前記プリペイドカードのセキュリティデータを読み出すセキュリティデータ読み出し部と、

利用者のセキュリティデータが入力される第２セキュリティデータ入力部と、

前記データ格納手段から取り込んだセキュリティデータと、前記プリペイドカードから読み出したセキュリティデータと、前記第２セキュリティデータ入力部から入力されたセキュリティデータとを照合し、それら３つのセキュリティデータが合致した場合にだけプリペイドカードの使用を許可する比較制御部とを備えたことを特徴とするプリペイドカード照合システム。

【請求項３】　請求項１または２記載のプリペイドカード照合システムにおいて、前記第１、第２セキュリティデータ入力部から入力されるセキュリティデータが、利用者の指紋情報、およびパスワードであり、前記データ格納手段に格納されるセキュリティデータが、前記第１セキュリティデータ入力部から入力された利用者の指紋情報、パスワード、ならびに前記データ読み出し部に読み出された前記プリペイドカードの認識番号であることを特徴とするプリペイドカード照合システム。

【請求項４】　ネットワークに接続され、電子遊技施設で使用されるプリペイドカードを購入する際に、利用者により入力されたセキュリティデータを前記プリペイドカードに書き込んで発行するプリペイドカード発行手段と、

前記ネットワークに接続され、前記ネットワークを介して前記プリペイドカード発行手段から入力されたセキュリティデータを格納するデータ格納手段と、

前記ネットワークに接続され、利用者が電子遊技施設において前記プリペイドカードを使用する際に入力されるセキュリティデータと前記ネットワークを介して前記プリペイドカード発行手段から取り込んだセキュリティデータと前記ネットワークを介して前記データ格納手段から取り込んだセキュリティデータとを照合し、それら３つのセキュリティデータが合致した場合にだけプリペイドカードの使用を許可するカード使用手段を設けた電子遊技機と備えたことを特徴とする電子遊技管理システム。

【請求項５】　請求項４記載の電子遊技管理システムにおいて、

前記プリペイドカード発行手段が、

利用者のセキュリティデータが入力される第１セキュリティデータ入力部と、

前記プリペイドカードに予め格納された認識番号を読み出すデータ読み出し部と、

前記第１セキュリティデータ入力部から入力されたセキュリティデータを前記プリペイドカードに書き込むデータ書き込み部とを備え、

前記カード使用手段が、

前記プリペイドカードのセキュリティデータを読み出すセキュリティデータ読み出し部と、

利用者のセキュリティデータが入力される第２セキュリティデータ入力部と、

前記データ格納手段から取り込んだセキュリティデータと、前記プリペイドカードから読み出したセキュリティデータと、前記第２セキュリティデータ入力部から入力されたセキュリティデータとを照合し、それら３つのセキュリティデータが合致した場合にだけプリペイドカードの使用を許可する比較制御部とを備えたことを特徴とする電子遊技管理システム。

【請求項６】　請求項４または５記載の電子遊技管理システムにおいて、前記第１、第２セキュリティデータ入力部から入力されるセキュリティデータが、利用者の指紋情報、およびパスワードであり、前記データ格納手段に格納されるセキュリティデータが、前記第１セキュリティデータ入力部から入力された利用者の指紋情報、パスワード、ならびに前記データ読み出し部により読み出された前記プリペイドカードの認識番号であることを特徴とする電子遊技管理システム。

【請求項７】　請求項４～６のいずれか１項に記載の電子遊技管理システムにおいて、

前記電子遊技管理システムに、前記ネットワークに接続

され、前記ネットワークを介して検知信号が入力された際に、前記電子遊技機に格納されている遊技プログラムを診断する診断プログラムを返信するセキュリティ制御手段を備え、
前記電子遊技機には、前記電子遊技機に電源が供給されたことを検知し、前記ネットワークを介して前記セキュリティに検知信号を出力し、前記セキュリティ制御手段から返送された診断プログラムにより遊技プログラムを診断し、診断結果に不具合がある場合に前記セキュリティ制御手段に異常信号を出力する検知制御部を設けたことを特徴とする電子遊技管理システム。
【請求項8】 請求項7記載の電子遊技管理システムにおいて、前記検知制御部は、前記セキュリティ制御手段から返信される診断プログラムを診断終了毎に消去することを特徴とする電子遊技管理システム。
【請求項9】 ネットワークに接続され、前記ネットワークを介して検知信号が入力された際に、電子遊技機に格納されている遊技プログラムを診断する診断プログラムを返信するセキュリティ制御手段と、
前記電子遊技機に電源が供給されたことを検知し、前記ネットワークを介して前記セキュリティに検知信号を出力し、前記セキュリティ制御手段から返送された診断プログラムにより遊技プログラムを診断し、診断結果に不具合がある場合に前記セキュリティ制御手段に異常信号を出力する検知制御部を設けた電子遊技機とを備えたことを特徴とする電子遊技管理システム。
【請求項10】 請求項9記載の電子遊技管理システムにおいて、前記検知制御部は、前記セキュリティ制御手段から返信される診断プログラムを診断終了毎に消去し、セキュリティ制御手段は、診断プログラムの内容を返信する毎に変更することを特徴とする電子遊技管理システム。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、プリペイドカードの不正使用防止技術に関し、特に、電子遊技施設などに用いられるＩＣカードの利用者照合に適用して有効な技術に関するものである。
【0002】
【従来の技術】たとえば、パチンコなどの遊技施設において、利用者が遊技玉の貸し出しを受ける場合として、予め購入したプリペイドカードを用いることが広く知られている。
【0003】本発明者が検討したところによれば、プリペイドカードは、たとえば、遊技施設内の券売機などで発売されている。利用者は、券売機から希望金額のプリペイドカードを購入した後、遊技機に設けられたカードユニットに該プリペイドカードを差し込み、遊技機の玉貸しボタンを押すことによって自動的に遊技玉が貸し出される。
【0004】また、遊技機は、一般的に利用者の操作に応じて内部に設けられたＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）などに記憶された遊技プログラムに従ってゲームが進行される。
【0005】
【発明が解決しようとする課題】ところが、上記のようなプリペイドカードによる遊技玉の貸し出し技術では、次のような問題点があることが本発明者により見い出された。
【0006】すなわち、プリペイドカードでは、使用者が該プリペイドカードを購入した本人か否かを確認できないために、たとえば、プリペイドカードを紛失した場合などに他人に使用されてしまう恐れがある。
【0007】また、プリペイドカードは、一般的に磁気カードであり、残高などの様々なデータが磁気データとして記憶されている。このため。磁気データが改竄されたプリペイドカードが不正使用されてしまう恐れもある。
【0008】さらに、遊技機は、前述のように遊技プログラムに従ってゲームが進行するので、たとえば、ある特定の操作を行った際に大当たり状態とするなどの不正なプログラム修正がされた場合などは、不正行為が行われていることを見分けることが困難となっている。
【0009】本発明の目的は、他人によるプリペイドカードの不正使用を確実に防止し、かつ電子遊技機の不正行為を効果的に抑制することができるプリペイドカード照合システムおよび電子遊技管理システムを提供することにある。
【0010】
【課題を解決するための手段】本発明のプリペイドカード照合システムは、ネットワークに接続され、プリペイドカードを購入する際に、利用者により入力されたセキュリティデータを該プリペイドカードに書き込んで発行するプリペイドカード発行手段と、ネットワークに接続され、そのネットワークを介してプリペイドカード発行手段から入力されたセキュリティデータを格納するデータ格納手段と、ネットワークに接続され、利用者がプリペイドカードを使用する際に入力されるセキュリティデータとネットワークを介してプリペイドカード発行手段から取り込んだセキュリティデータとネットワークを介して前記データ格納手段から取り込んだセキュリティデータとを照合し、それら３つのセキュリティデータが合致した場合にだけプリペイドカードの使用を許可するカード使用手段とを備えたことを特徴とする。
【0011】また、本発明のプリペイドカード照合システムは、前記プリペイドカード発行手段が、利用者のセキュリティデータが入力される第１セキュリティデータ入力部と、プリペイドカードに予め格納された認識番号を読み出すデータ読み出し部と、第１セキュリティデータ入力部から入力されたセキュリティデータを前記プリ

ペイドカードに書き込むデータ書き込み部とを備え、前記カード使用手段が、プリペイドカードのセキュリティデータを読み出すセキュリティデータ読み出し部と、利用者のセキュリティデータが入力される第2セキュリティデータ入力部と、データ格納手段から取り込んだセキュリティデータと、プリペイドカードから読み出したセキュリティデータと、第2セキュリティデータ入力部から入力されたセキュリティデータとを照合し、それら3つのセキュリティデータが合致した場合にだけプリペイドカードの使用を許可する比較制御部とを備えたことを特徴とする。

【0012】さらに、本発明のプリペイドカード照合システムは、前記第1、第2セキュリティデータ入力部から入力されるセキュリティデータが、利用者の指紋情報、およびパスワードであり、前記データ格納手段に格納されるセキュリティデータが、第1セキュリティデータ入力部から入力された利用者の指紋情報、パスワード、ならびにデータ読み出し部に読み出されたプリペイドカードの認識番号であることを特徴とする。

【0013】また、本発明の電子遊技管理システムは、ネットワークに接続され、電子遊技施設で使用されるプリペイドカードを購入する際に、利用者により入力されたセキュリティデータをプリペイドカードに書き込んで発行するプリペイドカード発行手段と、ネットワークに接続され、そのネットワークを介してプリペイドカード発行手段から入力されたセキュリティデータを格納するデータ格納手段と、ネットワークに接続され、利用者が電子遊技施設においてプリペイドカードを使用する際に入力されるセキュリティデータとネットワークを介してプリペイドカード発行手段から取り込んだセキュリティデータとネットワークを介してデータ格納手段から取り込んだセキュリティデータとを照合し、それら3つのセキュリティデータが合致した場合にだけプリペイドカードの使用を許可するカード使用手段を設けた電子遊技機と備えたことを特徴とする。

【0014】さらに、本発明の電子遊技管理システムは、前記プリペイドカード発行手段が、利用者のセキュリティデータが入力される第1セキュリティデータ入力部と、プリペイドカードに予め格納された認識番号を読み出すデータ読み出し部と、第1セキュリティデータ入力部から入力されたセキュリティデータをプリペイドカードに書き込むデータ書き込み部とを備え、前記カード使用手段が、プリペイドカードのセキュリティデータを読み出すセキュリティデータ読み出し部と、利用者のセキュリティデータが入力される第2セキュリティデータ入力部と、データ格納手段から取り込んだセキュリティデータとプリペイドカードから読み出したセキュリティデータと第2セキュリティデータ入力部から入力されたセキュリティデータとを照合し、それら3つのセキュリティデータが合致した場合にだけプリペイドカードの使用を許可する比較制御部とを備えたことを特徴とする。

【0015】また、本発明の電子遊技管理システムは、前記第1、第2セキュリティデータ入力部から入力されるセキュリティデータが、利用者の指紋情報、およびパスワードであり、前記データ格納手段に格納されるセキュリティデータが、第1セキュリティデータ入力部から入力された利用者の指紋情報、パスワード、ならびにデータ読み出し部により読み出されたプリペイドカードの認識番号であることを特徴とする。

【0016】さらに、本発明の電子遊技管理システムは、前記電子遊技管理システムに、ネットワークに接続され、ネットワークを介して検知信号が入力された際に、電子遊技機に格納されている遊技プログラムを診断する診断プログラムを返信するセキュリティ制御手段を備え、前記電子遊技機には、電子遊技機に電源が供給されたことを検知し、ネットワークを介してセキュリティに検知信号を出力し、セキュリティ制御手段から返送された診断プログラムにより遊技プログラムを診断し、診断結果に不具合がある場合にセキュリティ制御手段に異常信号を出力する検知制御部を設けたことを特徴とする。

【0017】また、本発明の電子遊技管理システムは、前記検知制御部は、セキュリティ制御手段から返信される診断プログラムを診断終了毎に消去することを特徴とする。

【0018】さらに、本発明の電子遊技管理システムは、ネットワークに接続され、そのネットワークを介して検知信号が入力された際に、電子遊技機に格納されている遊技プログラムを診断する診断プログラムを返信するセキュリティ制御手段と、電子遊技機に電源が供給されたことを検知し、ネットワークを介してセキュリティに検知信号を出力し、セキュリティ制御手段から返送された診断プログラムにより遊技プログラムを診断し、診断結果に不具合がある場合に該セキュリティ制御手段に異常信号を出力する検知制御部を設けた電子遊技機とを備えたことを特徴とする。

【0019】また、本発明の電子遊技管理システムは、前記検知制御部は、セキュリティ制御手段から返信される診断プログラムを診断終了毎に消去し、セキュリティ制御手段は、診断プログラムの内容を返信する毎に変更することを特徴とする。

【0020】以上のことにより、プリペイドカードを使用する際に、3つのセキュリティデータよって照合するので、該プリペイドカードの不正使用を、短時間で確実に防止することができる。

【0021】また、電子遊技機に電源が供給されると診断プログラムによって、遊技プログラムを自動診断するので、作業工数などをかけることなく、遊技プログラムの不正使用などを発見、防止することができる。

【0022】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。

【００２３】図１は、本発明の一実施の形態による電子遊技システムにおける構成の説明図、図２は、本発明の一実施の形態による電子遊技システムにおける電子遊技機の説明図、図３は、本発明の一実施の形態によるプリペイドカード販売機からＩＣカードを購入する際の電子遊技システムにおけるフローチャート、図４は、本発明の一実施の形態による利用者が電子遊技機によりプレイする際の電子遊技システムにおけるフローチャート、図５は、本発明の一実施の形態による電子遊技機のセキュリティチェックを行う際の電子遊技システムにおけるフローチャートである。

【００２４】本実施の形態において、電子遊技システム（電子遊技管理システム）１は、図１に示すように、複数の電子遊技機（プリペイドカード照合システム、カード使用手段）２、管理コンピュータ３、セキュリティコンピュータ（セキュリティ制御手段）４、カード管理運営コンピュータ（プリペイドカード照合システム、データ格納手段）５、ならびにプリペイドカード販売機（プリペイドカード照合システム、プリペイドカード発行手段）６から構成されている。

【００２５】また、電子遊技システム１のうち、複数の電子遊技機２、管理コンピュータ３、およびプリペイドカード販売機６は、電子遊技施設内に設けられている。セキュリティコンピュータ４は、電子遊技機２のプログラムなどのセキュリティ管理を行う機関が有しており、カード管理運営コンピュータ５は、ＩＣカード（プリペイドカード）７を発行するカード発行機関などが有している。これらはセキュリティコンピュータ４、カード管理運営コンピュータ５は、電子遊技施設外に設けられており、他の電子遊技施設に設けられている電子遊技機とも接続されている。

【００２６】電子遊技機２は、格納された遊技プログラムに基づいてゲームが進行するものであり、利用者が後述するＩＣカード７を利用して遊技するものであり、ゲーム結果に応じた価値が付与される。

【００２７】ＩＣカード７は、たとえば、カードの中に半導体チップと、それに接続するアンテナとが組み込まれた構成からなり、このアンテナがユニット、およびカードの中の半導体チップから発射する電波をとらえ、カード内の情報のやりとりをする。

【００２８】また、ＩＣカード７には、利用者が購入時に入力するセキュリティデータ、および管理データなどが格納される。セキュリティデータは、利用者が入力するパスワード、ＩＣカードに予め格納されている識別番号（またはＩＣカード７の製造番号、固有番号など）、および指紋情報などであり、管理データは、カードポイントなどである。

【００２９】電子遊技機２には、専用回線、電話回線などの回線（ネットワーク）Ｋ１を介してセキュリティコンピュータ４がオンラインに接続されており、電子遊技機２のプログラム不正などを診断する診断プログラムなどのデータのやり取りが行われる。

【００３０】また、電子遊技機２には、ＬＡＮなどの回線Ｋ２を介して管理コンピュータ３が、それぞれ接続されている。管理コンピュータ３は、電子遊技機２の稼働率、売り上げなどの管理集計を司り、セキュリティコンピュータ４は、電子遊技機２の使用状況を監視し、不正使用を防止する。

【００３１】カード管理運営コンピュータ５にも回線Ｋ１が接続されており、このカード管理運営コンピュータ５は、利用者がＩＣカード７を購入する際に、入力されるセキュリティデータ、および管理データなどを格納する。

【００３２】プリペイドカード販売機６には、専用回線、あるいは電話回線などの回線（ネットワーク）Ｋ３を介してカード管理運営コンピュータ５が接続されている。このプリペイドカード販売機６には、指紋センサ（第１セキュリティデータ入力部）、入力部（第１セキュリティデータ入力部）、データ読み出し／書き込み機能（データ読み出し部、データ書き込み部）が備えられ、かつ入力されたセキュリティデータ、および管理データをカード管理運営コンピュータ５に出力する機能も備えている。

【００３３】指紋センサは、利用者がＩＣカード７を購入する際に利用者自身の指紋を指紋情報として取り込む。入力部は、ディスプレイとキーボード、あるいはそれらが一体となったタッチ入力パネルなどからなり、同じく利用者がＩＣカード７を購入する際にパスワードなどの情報を入力する。データ読み出し／書き込み機能は、ＩＣカード７にセキュリティデータなどを書き込んだり、管理データを読み出したりする機能である。

【００３４】さらに、電子遊技機２の回路構成について説明する。

【００３５】電子遊技機２は、図２に示すように、指紋センサ（第２セキュリティデータ入力部）８、カードリード／ライト部（セキュリティデータ読み出し部）９、パスワード入力部（第２セキュリティデータ入力部）１０、セキュリティ通信制御部（比較制御部、検知制御部）１１、遊技メインコントロール部１２、遊技プログラム格納メディアドライブ１３、Ｉ／Ｏ部１４、電源ユニット１５、表示部１６、ならびにスイッチパネル部１７から構成されている。

【００３６】指紋センサ８、およびカードリード／ライト部９には、セキュリティ通信制御部１１が接続されている。指紋センサ８は、利用者の指紋などの指紋情報として取り込む。カードリード／ライト部９は、ＩＣカード７に記憶されているデータを読み出したり、書き込んだりする。

【００３７】セキュリティ通信制御部１１は、回線Ｋ１を介してセキュリティコンピュータ４、およびカード管理運営コンピュータ５に接続されている。セキュリティ通信制御部１１は、ＩＣカード７、指紋センサ８、セキュリティデータの照合結果、あるいはセキュリティコンピュータ４から出力される診断プログラムの診断結果に基づいて遊技メインコントロール部１１の動作制御を行う。

【００３８】遊技メインコントロール部１２には、セキュリティ通信制御部１１、遊技プログラム格納メディアドライブ１３、ならびにＩ／Ｏ部１４などが接続されている。

【００３９】遊技メインコントロール部１２は、遊技プログラムに基づいて電子遊技機２のゲーム進行などの制御を司る。遊技プログラム格納メディアドライブ１３は、たとえば、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｃ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）ドライブ、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｉｄｅｏ Ｄｉｓｃ）－ＲＯＭドライブなどであり、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭなどに記録された遊技プログラムを読み出す。Ｉ／Ｏ部１４には、管理コンピュータ３が接続されており、このＩ／Ｏ部１４を介してデータが入出力される。

【００４０】電源ユニット１５は、指紋センサ８、カードリード／ライト部９、セキュリティ通信制御部１１、遊技メインコントロール部１２、遊技プログラム格納メディアドライブ１３、Ｉ／Ｏ部１４、表示部１６、およびスイッチパネル部１７に最適な電源を供給するとともに、電子遊技機２に電源が投入された際に起動信号をセキュリティ通信制御部１１に出力する。

【００４１】表示部１６、およびスイッチパネル部１７には、遊技メインコントロール部１２がそれぞれ接続されている。表示部１６は、たとえば、液晶ディスプレイ、ブラウン管などからなり、ゲームプレイ用の画像が表示される。スイッチパネル部１８は、ゲームプレイ用のスイッチやデータ入力用のキーボードなどの操作部が備えられている。

【００４２】次に、本実施の形態における電子遊技システムの動作について、図１、図２、および図３～図５のフローチャートを用いて説明する。

【００４３】まず、利用者がＩＣカードを購入する際には、図３に示すように、プリペイドカード販売機６に代金を投入し、プリペイドカード販売機６に備えられた指紋センサに利用者自身の指を押しつけて指紋情報を入力し、プリペイドカード販売機６の入力部からパスワードを入力する（ステップＳ１０１）。

【００４４】入力された利用者の指紋情報、パスワードは、プリペイドカード販売機６のデータ読み出し／書き込み機能によってＩＣカード７に書き込まれ、個々のＩＣカード７に予めそれぞれ付与された認識番号とともにセキュリティデータとして記憶される（ステップＳ１０２）。

【００４５】また、ＩＣカード７には、プリペイドカード販売機６のデータ読み出し／書き込み機能により利用者が希望（購入）する任意のポイントデータが記憶される（ステップＳ１０２）。

【００４６】同時に、プリペイドカード販売機６は、データ読み出し／書き込み機能によってＩＣカード７の認識番号を読み出し、この認識番号、利用者の指紋情報、ならびにパスワードからなるセキュリティデータをカード管理運営コンピュータ５に出力する。

【００４７】カード管理運営コンピュータ５は、送信されたセキュリティデータをデータベースなどに格納する（ステップＳ１０３）。これらの動作が終了すると、プリペイドカード販売機６からＩＣカード７が発行される（ステップＳ１０４）。

【００４８】利用者が電子遊技機２によりプレイする際には、図４に示すように、購入したＩＣカード７を電子遊技機２のカードリード／ライト部９に差し込むとともに、ＩＣカード７の購入時に登録した指紋と同じ指を遊技機２の指紋センサ８に押しつける（ステップＳ２０１）。

【００４９】カードリード／ライト部９は、差し込まれたＩＣカード７からセキュリティデータ、ならびに管理データを読み出し、セキュリティ通信制御部１０に出力する（ステップＳ２０２）。

【００５０】指紋センサ８は、利用者の指紋情報を取り込み、セキュリティ通信制御部１０に出力する（ステップＳ２０３）。また、利用者は、電子遊技機２のパスワード入力部１０からＩＣカード７を購入した際に入力したパスワードを入力する（ステップＳ２０４）。

【００５１】このとき、セキュリティ通信制御部１０は、カード管理運営コンピュータ５のデータベースから、プリペイドカード販売機６から入力されたセキュリティデータを取り込む（ステップＳ２０５）。ここで、ステップＳ２０２～Ｓ２０５の処理は、処理の順番が入れ替わったり、あるいはすべてを同時に処理するようにしてもよい。

【００５２】そして、セキュリティ通信制御部１０は、電子遊技機２から入力されたセキュリティデータ（指紋センサ８が取り込んだ指紋情報、パスワード入力部１０から入力されたパスワード）、カードリード／ライト部９が読み出したＩＣカード７のセキュリティデータ、ならびにカード管理運営コンピュータ５のデータベースから取り込んだセキュリティデータを照合する（ステップＳ２０６）。

【００５３】これらすべてのセキュリティデータが合致している場合には、利用者が本人であることを認証し、セキュリティ通信制御部１０は、ＩＣカード７の使用を許可し、遊技メインコントロール部１２にゲームを開始する制御信号を出力する（ステップＳ２０７）。

【００５４】この信号を受けて遊技メインコントロール部１２は、遊技用のポイントを要求する。さらに、ステップＳ２０７の処理において、セキュリティデータが一致しない場合には、セキュリティ通信制御部１０が、そのＩＣカード７をカードリード／ライト部９から強制的に排出するように制御する（ステップＳ２０８）。

【００５５】遊技用のポイントが要求されると利用者は、任意のポイントをスイッチパネル部１９などから投入指示し（ステップＳ２０９）、ゲームが開始となる。

【００５６】利用者から投入指示されたポイントは、セキュリティ通信制御部１１を介してカード管理運営コンピュータ５に送信され、カード管理運営コンピュータ５のデータベースに格納された管理データ、およびＩＣカード７の管理データから投入指示されたポイントが減算される。プレイ中に遊技用のポイントがなくなった場合には、再び利用者が任意のポイントをスイッチパネル部１９などから投入指示する。

【００５７】また、ゲームを終了する際には、スイッチパネル部１７などに設けられた精算ボタンを押すことによって、最終的なポイントの精算処理が行われ、精算処理後のポイントが、ＩＣカード７、ならびにカード管理運営コンピュータ５のデータベースに新たに書き換えられる。

【００５８】次に、電子遊技施設の開店時における電子遊技機２のセキュリティチェックについて、図５を用いて説明する。

【００５９】電子遊技機２に電源が投入されると（ステップＳ３０１）、電源ユニット１５から起動信号がセキュリティ通信制御部１１に出力される。セキュリティ通信制御部１１は、起動信号に基づいて電子遊技機２に電源投入されたことをセキュリティコンピュータ４に知らせる検知信号を出力する（ステップＳ３０２）。

【００６０】その検知信号を受けたセキュリティコンピュータ４は、セキュリティ通信制御部１１に診断プログラムを送信し（ステップＳ３０３）、その診断プログラムによって遊技プログラムに不正が施されて否かを診断する（ステップＳ３０４）。

【００６１】この診断プログラムは、毎日プログラム内容を書き換えて送信されており、この診断プログラムに対応した不正プログラムを開発することを事実上不可能とすることができる。

【００６２】診断プログラムによる遊技プログラムの診断において、不正がないと診断されると、診断プログラムはセキュリティ通信制御部１１によって自動的に消去され（ステップＳ３０５）、電子遊技機２がゲーム開始が可能状態となる。

【００６３】また、遊技プログラムに不正があると判断されると、セキュリティ通信制御部１１は、不正検出信号をセキュリティコンピュータ４に出力するとともに、遊技メインコントロール部１２が動作しないように制御を行う（ステップＳ３０６）。不正検出信号を受けたセキュリティコンピュータ４は、不正対策の関係機関などに通報する（ステップＳ３０７）。

【００６４】さらに、セキュリティ通信制御部１１は、遊技プログラム格納メディアドライブ１３に格納されたＣＤ－ＲＯＭなどが不正に取り出された際にも、遊技プログラム格納メディアドライブ１３から出力される検出信号に基づいてセキュリティコンピュータ４に不正検出信号を出力する。

【００６５】それにより、本実施の形態によれば、ＩＣカード７の利用者を、電子遊技機２から入力されたセキュリティデータ、カード管理運営コンピュータ５に格納されているセキュリティデータ、ならびにＩＣカード７に格納されたセキュリティデータの３つによって照合するので、ＩＣカード７をリアルタイムに管理でき、かつ不正使用を短時間で効率よく防止することができる。

【００６６】また、日替わりの診断プログラムによって、電子遊技機２の電源投入時に毎日遊技プログラムに不正が施されていないかを自動的に診断することにより、作業工数をかけることなく、遊技プログラムの不正使用を防止することができる。

【００６７】本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【００６８】たとえば、前記実施の形態においては、カード使用手段としてゲーム結果に応じた価値（ポイント）が付与される、いわゆるポイント加減算タイプの電子遊技機を用いた場合について記載したが、インターネットなどにみられる使用時間に比例してポイントが減算されるサービス、あるいは、ポイントによるショッピングなどのポイント減算タイプのシステムにカード使用手段を用いるようにしてもよい。

【００６９】

【発明の効果】（１）本発明によれば、プリペイドカードを使用する際に、３つのセキュリティデータを照合するので、該プリペイドカードをリアルタイムに管理しながら不正使用を短時間で確実に防止することができる。（２）また、本発明では、電子遊技機に電源が供給される毎に診断プログラムによって遊技プログラムを自動診断するので、作業工数などをかけることなく、遊技プログラムの改竄、不正使用などを確実に防止することができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態による電子遊技システムにおける構成の説明図である。

【図２】本発明の一実施の形態による電子遊技システムにおける電子遊技機の説明図である。

【図３】本発明の一実施の形態によるプリペイドカード販売機からＩＣカードを購入する際の電子遊技システムにおけるフローチャートである。

【図4】本発明の一実施の形態による利用者が電子遊技機によりプレイする際の電子遊技システムにおけるフローチャートである。

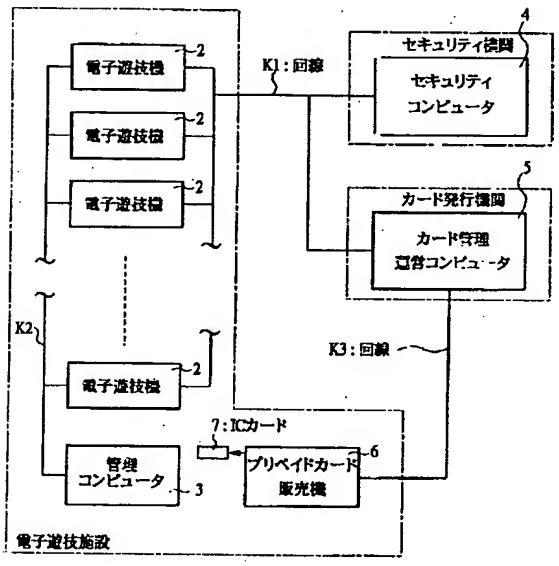
【図5】本発明の一実施の形態による電子遊技機のセキュリティチェックを行う際の電子遊技システムにおけるフローチャートである。

【符号の説明】

1　電子遊技システム（電子遊技管理システム）
2　電子遊技機（プリペイドカード照合システム、カード使用手段）
3　管理コンピュータ
4　セキュリティコンピュータ（セキュリティ制御手段）
5　カード管理運営コンピュータ（プリペイドカード照合システム、データ格納手段）
6　プリペイドカード販売機（プリペイドカード照合システム、プリペイドカード発行手段）
7　ICカード（プリペイドカード）
8　指紋センサ（第2セキュリティデータ入力部）
9　カードリード／ライト部（セキュリティデータ読み出し部）
10　パスワード入力部（第2セキュリティデータ入力部）
11　セキュリティ通信制御部（比較制御部、検知制御部）
12　遊技メインコントロール部
13　遊技プログラム格納メディアドライブ
14　I／O部
15　電源ユニット
16　表示部
17　スイッチパネル部
K1　回線（ネットワーク）
K2　回線
K3　回線（ネットワーク）

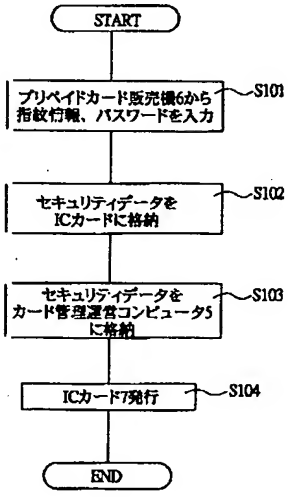
【図1】

図 1



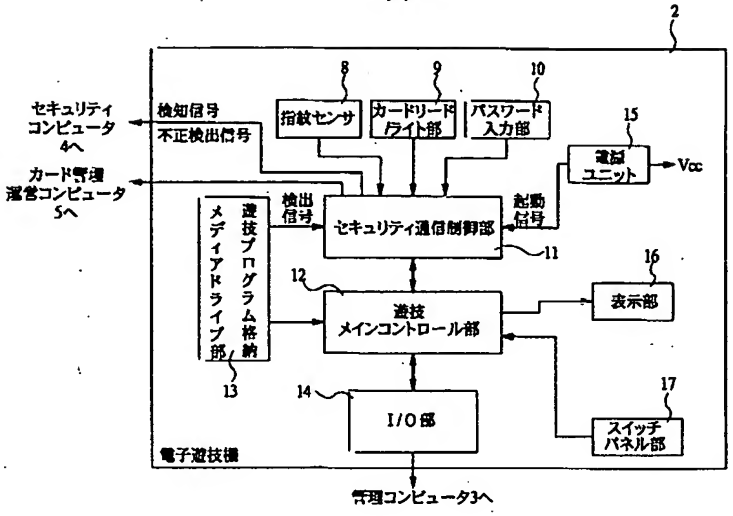
【図3】

図 3



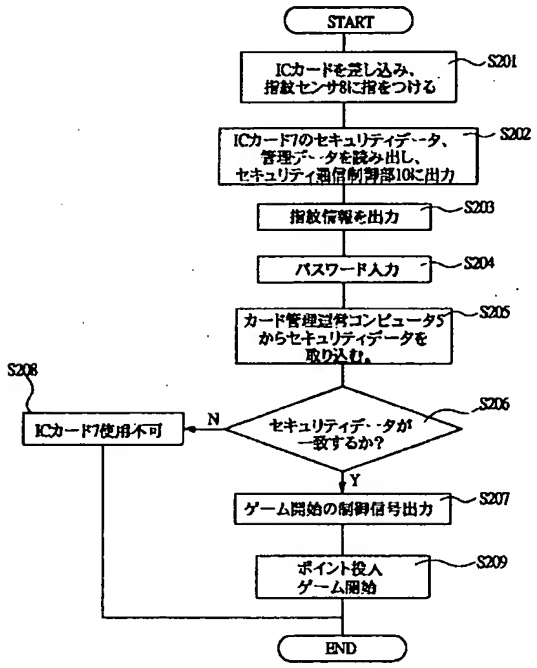
【図2】

図 2



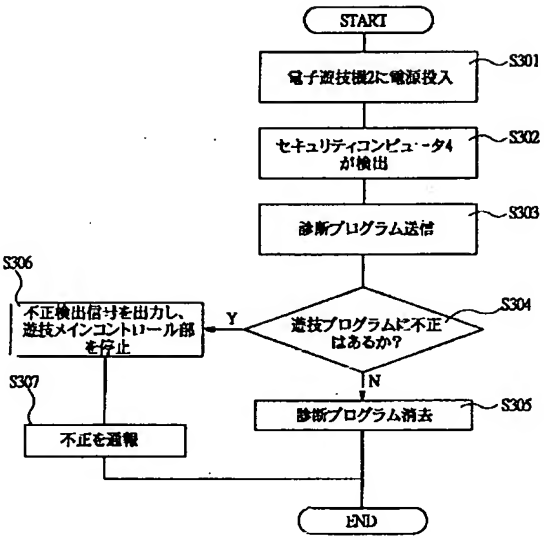
【図4】

図 4



【図5】

図 5



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		(参考)
G06K 17/00		G06K 17/00	T	
G07F 7/12		G07F 7/08	C	

Fターム(参考) 2C088 BB15 BB43 CA31
3E044 AA05 BA06 DA05
5B055 HA02 HA04 HA06 HB02 JJ05
KK05 KK07
5B058 CA27 KA02 KA04 KA06 KA11
KA33 KA38 YA06